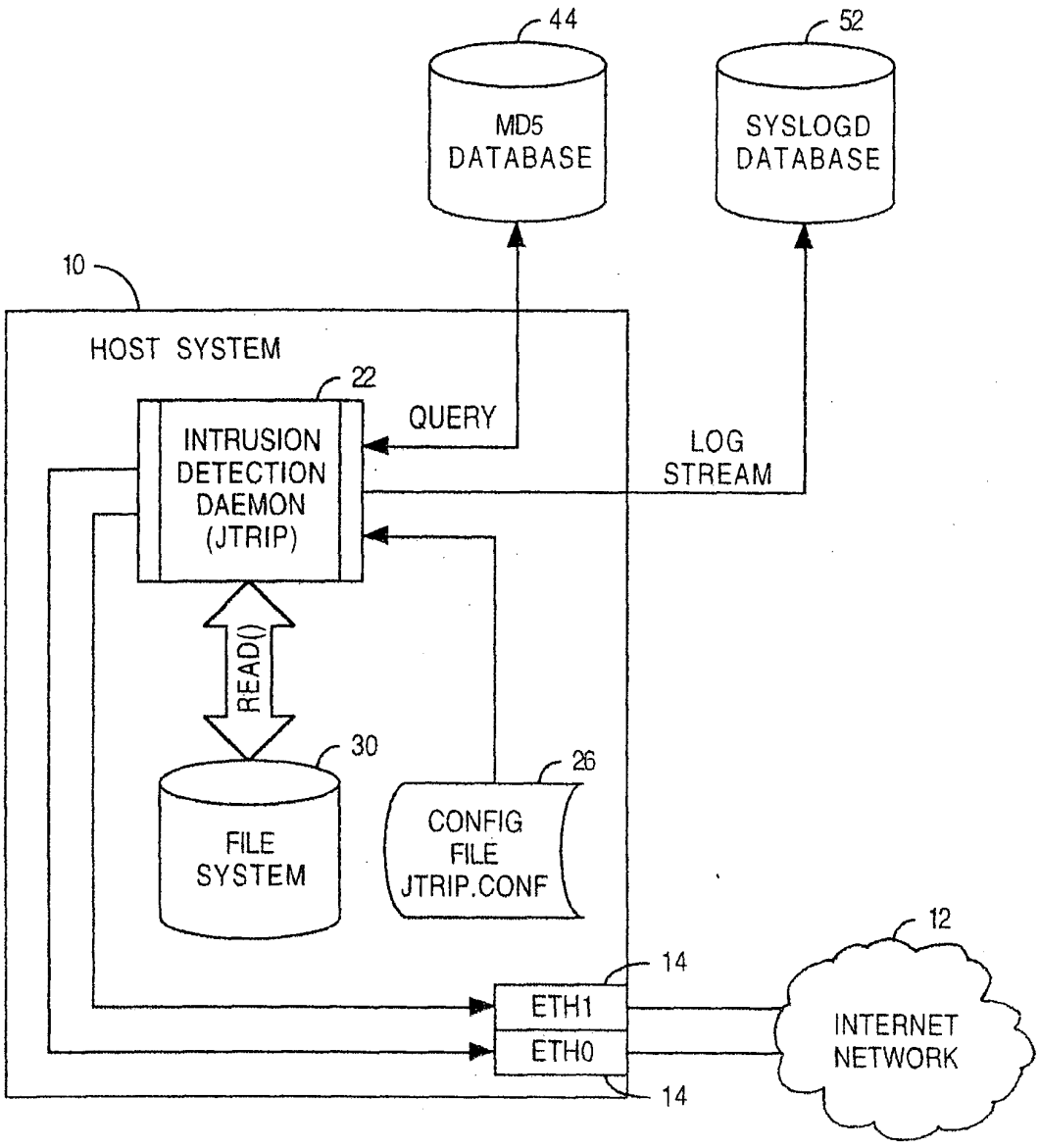
44
MD5
DATABASE
52
SYSLOGD
DATABASE
10
HOST SYSTEM
22
INTRUSION
DETECTION
DAEMON
(JTRIP)
QUERY
LOG
STREAM
READ()
30
FILE
SYSTEM
26
CONFIG
FILE
JTRIP.CONF
12
14
ETH1
ETH0
INTERNET
NETWORK
14

FIG. 1

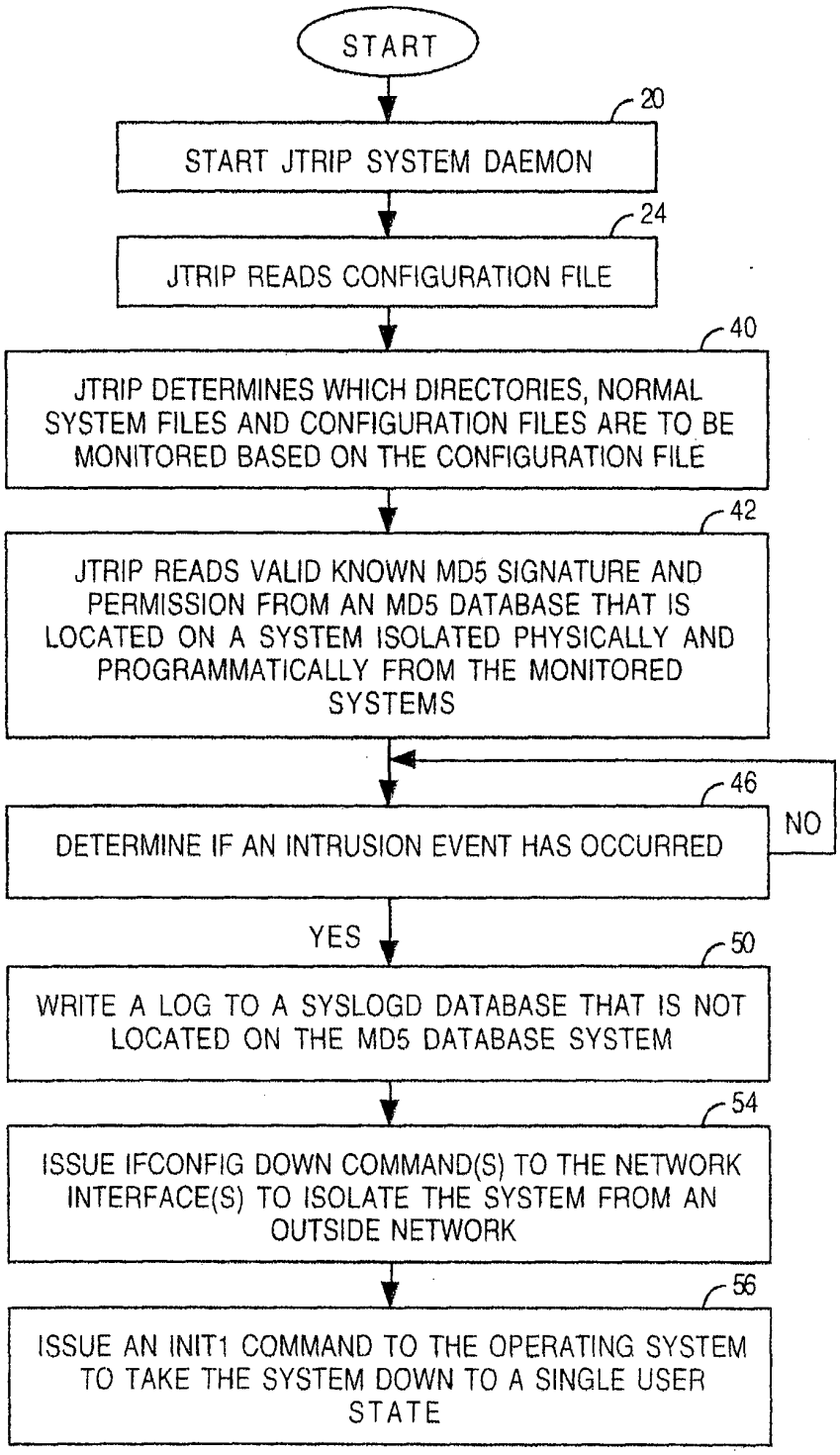
START
20
START JTRIP SYSTEM DAEMON
24
JTRIP READS CONFIGURATION FILE
40
JTRIP DETERMINES WHICH DIRECTORIES, NORMAL SYSTEM FILES AND CONFIGURATION FILES ARE TO BE MONITORED BASED ON THE CONFIGURATION FILE
42
JTRIP READS VALID KNOWN MD5 SIGNATURE AND PERMISSION FROM AN MD5 DATABASE THAT IS LOCATED ON A SYSTEM ISOLATED PHYSICALLY AND PROGRAMMATICALLY FROM THE MONITORED SYSTEMS
46
DETERMINE IF AN INTRUSION EVENT HAS OCCURRED
NO
YES
50
WRITE A LOG TO A SYSLOGD DATABASE THAT IS NOT LOCATED ON THE MD5 DATABASE SYSTEM
54
ISSUE IFCONFIG DOWN COMMAND(S) TO THE NETWORK INTERFACE(S) TO ISOLATE THE SYSTEM FROM AN OUTSIDE NETWORK
56
ISSUE AN INIT1 COMMAND TO THE OPERATING SYSTEM TO TAKE THE SYSTEM DOWN TO A SINGLE USER STATE

FIG. 2

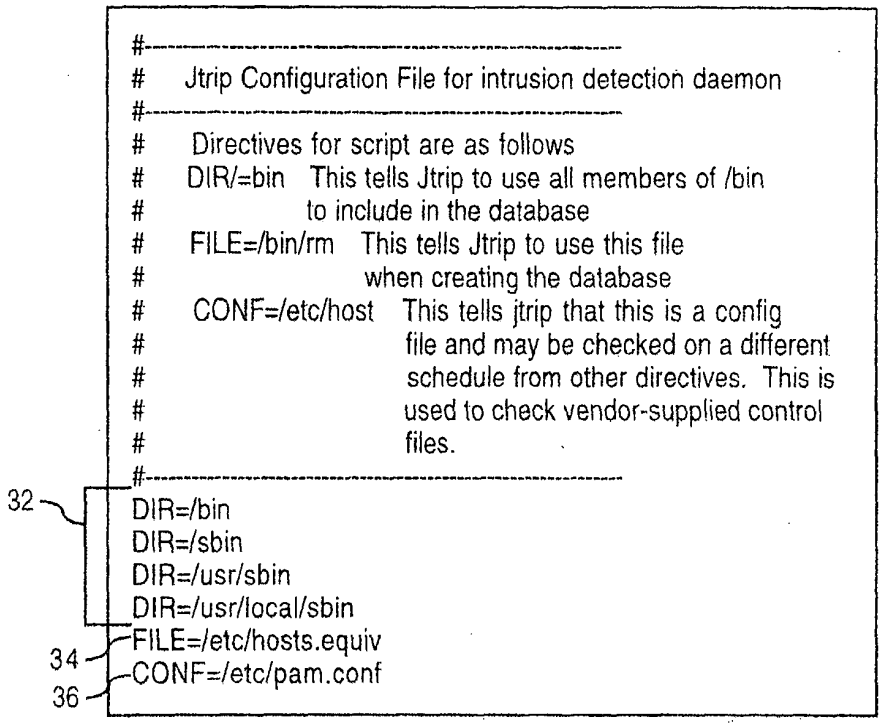
#----------
Jtrip Configuration File for intrusion detection daemon
#----------
Directives for script are as follows
DIR/=bin This tells Jtrip to use all members of /bin
to include in the database
FILE=/bin/rm This tells Jtrip to use this file
when creating the database
CONF=/etc/host This tells jtrip that this is a config
file and may be checked on a different
schedule from other directives. This is
used to check vendor-supplied control
files.
#----------
32
DIR=/bin
DIR=/sbin
DIR=/usr/sbin
DIR=/usr/local/sbin
34
FILE=/etc/hosts.equiv
36
CONF=/etc/pam.conf

FIG. 3